

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN**

<p>ASSIYAH FATEEN, <i>on behalf of herself and all others similarly situated,</i></p> <p style="text-align: center;">Plaintiff,</p> <p>v.</p> <p>COREWELL HEALTH d/b/a BEAUMONT HEALTH,</p> <p style="text-align: center;">Defendant.</p>	<p>Case No. _____</p> <p>CLASS ACTION COMPLAINT</p> <p>JURY TRIAL DEMANDED</p>
---	--

CLASS ACTION COMPLAINT

1. Plaintiff Assiyah Fateen (“Plaintiff”), at all times relevant herein, has been a patient of Corewell Health, d/b/a Beaumont Health (“Beaumont” or “Defendant”), and brings this class action against Defendant in her individual capacity and on behalf of all others similarly situated, and alleges the following, upon personal knowledge as to her own actions, her counsels’ investigation, and upon information and belief as to all other matters.

NATURE OF THE ACTION

2. This class action lawsuit arises out of Beaumont’s unlawful use of third-party tracking technologies by data brokers such as Meta Platforms, Inc. d/b/a/ Meta (“Facebook”) and Google LLC (“Google”) to surreptitiously intercept and disclose its patients’ private and protected communications, including communications concerning highly sensitive personal health information, to third parties without patients’ knowledge or consent.

3. By purposely embedding and deploying third party tracking technologies on Beaumont’s web properties, Beaumont engages in the unauthorized disclosure of its patients’

highly sensitive Protected Health Information (“PHI”) and Personally Identifiable Information (“PII” and together with PHI, “Private Information”) to third parties including, but not limited to, Facebook and Google. Such disclosures of PHI and PII violate state and federal law.

4. Beaumont encourages patients and prospective patients to use its website, available at <https://www.beaumont.org/> (the “Website”) and its patient portal, available at <https://mybeaumontchart.com/mychart/Authentication/Login?> (the “Portal”), to communicate about symptoms and conditions, research treatments, lookup physicians, schedule appointments, pay their bills, among other activities.¹

5. Unbeknownst to its patients and prospective patients, their communications were intercepted and disclosed to third parties through Beaumont’s use of third-party tracking technologies such as the Meta Pixel (“Facebook Pixel” or “Pixel”), as well as Google Analytics, DoubleClick and Google Tag Manager (together with the Facebook Pixel, “Tracking Tools”), third party trackers from companies such as Facebook and Google.²

¹ Without the benefit of discovery, Plaintiff does not have the evidence that Beaumont installed third-party trackers on its Patient Portal; however, given that Defendant did choose to embed third-party tracking codes on the log-in pages for the Portal, as well as on the bill pay webpages, upon information and good faith belief Plaintiff alleges that Beaumont installed such trackers in the Portal as well. MyChart is run by a third party, Epic Software Systems (Epic), which permits its partners to deploy “custom analytics scripts.” Tracking technologies can be embedded into the code, and because of Defendant’s pervasive use of tracking technologies on its main page, upon information and belief Plaintiff avers that third-party tracking technologies were also deployed in Beaumont’s MyChart Portal.

² In addition to the Tracking Tools, upon information and belief Defendant also installed and implemented Facebook’s Conversions API (“CAPI”) on its Website servers. Unlike the Facebook Pixel which co-opts a website user’s browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user’s browser to transmit information directly to Facebook. Instead, CAPI tracks the user’s website interaction, including Private Information, records and stores that information on the website owner’s servers, and then transmits the data to Facebook from the website owner’s servers. See <https://revealbot.com/blog/facebook-conversions-api/>. Because CAPI is located on the website owner’s servers and is not a bug planted onto the website user’s browser, it allows website owners like Defendant to circumvent any ad

6. One of the Tracking Tools Beaumont deployed on its Website is the Facebook Pixel.³ The Pixel is a snippet of code that, when embedded on a website, tracks the website visitor's activity on that website and sends that data to a third party – here, to Meta.

7. The Pixel tracks and logs the pages a website user visits during a website session that reveals their patient status and other PII and PHI, searches, and other submissions to the website. Indeed, the Pixel is routinely used to target specific individuals by utilizing the data gathered through the Pixel to build profiles for the purpose of future targeting and marketing.

8. The information Beaumont transmitted to third parties, such as Meta, without Plaintiff's consent included PHI,⁴ which is some of the most personal and sensitive data Plaintiff has.

9. Additionally, when a patient communicates with Beaumont's Web Properties where the Pixel is present, Pixel source code causes the exact content of the patients' communications with the Website to be re-directed to Meta in a way that identifies the person as a patient.

blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly.

³ Meta also provides other tracking technologies that give the same or similar tracking functionalities as the Pixel including, but not limited to, Conversions API, SDKs, and Audiences. Absent discovery, Plaintiff is unable to independently confirm whether Defendant installed such tracking technologies on its Website.

⁴ Under HIPAA, "health information" is defined as "any information[], whether oral or recorded in any form or medium, that . . . [i]s created or received by a health care provider . . . and [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103. Additionally, HIPAA defines "health care" as "care, services, or supplies related to the health of an individual" and includes, but is not limited to, the "[s]ale or dispensing of drug, device, equipment, or other item in accordance with a prescription." *Id.*

10. Here, Plaintiff used the Website to communicate about her sensitive health conditions and symptoms, and to research potential treatments and physicians. Unbeknownst to Plaintiff, when she communicated about her PHI, the Pixel secretly intercepted, recorded, and transmitted those private communications to Meta along with unique identifiers Meta could use to identify Plaintiff.

11. As a result of Defendant's use of the Pixel, Plaintiff's and Class Members' PHI and PII including, but not limited to, unique personal identifiers, computer IP addresses, patient status, specific search terms, health conditions and symptoms, treatments, physicians, and appointment details, used to link the sensitive web communications to Plaintiff and Class Members, were compromised and disclosed to third parties such as Meta without authorization or consent.

12. Such private information allows Meta to know that a specific patient was seeking confidential health care or exploring treatment for a specific condition.

13. Defendant's Tracking Tools have also transmitted patients' PHI and PII to additional unauthorized third parties for marketing and advertising purposes, including Google, via tracking codes like Google Analytics, Google Tag Manager and DoubleClick.

14. Google's tracking technologies operate much like the Meta Pixel. As one District Court recently described:

Whenever a user visits a website that is running Google Analytics, Ad Manager, or some similar Google service, Google's software directs the user's browser to send a separate communication to Google. This happens even when users are in private browsing mode, unbeknownst to website developers or the users themselves. The operation is not in dispute. When a user visits a website, the user's browser sends a "GET" request to the website to retrieve it. This GET request contains the following information: the Request URL, or the URL of the specific webpage the user is trying to access; the user's IP address; the User-agent, which identifies the user's device platform and browser; user's geolocation, if available; the Referer, which is the URL of the page on which the user clicked a link to access a new page; event data, which describes how users interact with a website, for example, whether they saw an ad or played a video; and the actual search queries on the site. At the same

time, the user's browser reads Google's code, which is embedded on the website. Google's code instructs the user's browser to send a second and concurrent transmission directly to Google. This second transmission tells Google exactly what a user's browser communicated to the website.⁵

15. In secretly deploying the Tracking Tools on its Website to intercept and disclose website communications concerning its patients' and prospective patients' PHI and PII, Defendant acted with a tortious and criminal purpose in violation of state and federal laws.

16. Plaintiff and Class Members never consented to, authorized, or otherwise agreed to allow Defendant to disclose their PHI and PII to anyone other than those reasonably believed to be part of Beaumont, acting in some healthcare-related capacity. Despite this, Defendant knowingly and intentionally disclosed Plaintiff's and Class Members' PHI and PII to Meta, Google, and other third parties.

17. Given the nature of Meta and Google's businesses as two of the world's largest online advertising companies, Plaintiff's and Class Members' PHI and PII can and will likely be further used by or exposed to additional third parties.

18. As a direct and proximate result of Defendant's unauthorized exposure of Plaintiff's and Class Members' PHI and PII, Plaintiff and Class Members have suffered injury, including an invasion of privacy, loss of the benefit of the bargain Plaintiff and Class Members considered at the time they bargained for healthcare services and agreed to use Defendant's Website for services, statutory damages, and the continued and ongoing risk to their PHI and PII.

19. Plaintiff brings this action individually, and on behalf of a Class of similarly

⁵ *Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at *2 (N.D. Cal. Aug. 7, 2023). As explained by the Court in *Brown*, Google connects user data to IP addresses; IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifiable information that constitutes one of the 18 HIPAA identifiers of PHI. See 45 C.F.R. § 164.514 (2).

situated individuals, to recover for harms suffered and assert the following claims: (i) violations of the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2511; (ii) breach of fiduciary duty/confidentiality; (iii) invasion of privacy; (iv) Breach of Implied Contract; (v) Negligence; (vi) Unjust Enrichment; (vii) Violation of the Michigan Consumer Protection act, MCL 445.903 and (viii) violation of the Michigan Nonprofit Health Care Corporation Reform Act, MCL § 550.1406.

PARTIES

20. Plaintiff Assiyah Fateen is, and at all relevant times was a resident of Detroit, Wayne County in Michigan.

21. Defendant Beaumont is a Michigan-based health care provider with its principal place of business located at 100 Michigan Street, NE, Grand Rapids, Michigan, 49503.

22. In 2022, Beaumont merged with Spectrum Health of West Michigan to form Corewell Health.⁶ Beaumont currently operates under the Corewell Health umbrella.

23. Beaumont operates 1,778 licensed beds, 3,100 physicians, and three hospital systems.⁷

24. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 (HIPAA).

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under 28 U.S.C.

⁶ See <https://www.beaumont.org/health-wellness/press-releases/spectrum-health-and-beaumont-health-to-launch-new-health-system-on-feb-1> (last visited Oct. 25, 2024).

⁷ See <https://www.beaumont.org/about-us/history> (last visited Oct. 25, 2024).

§ 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.

26. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges one or more question(s) of federal law such as the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2511, *et seq.*

27. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff’s claims occurred in and emanated from this District.

28. Venue is proper under 28 U.S.C § 1391(b)(1) because Defendant’s principal place of business is in this District.

FACTUAL ALLEGATIONS

A. Federal Regulators Have Warned Healthcare Providers About the Impermissible Use of Tracking Technologies.

29. The surreptitious collection and disclosure of PHI and PII is a serious data security and privacy issue. Both the Federal Trade Commission (“FTC”) and HHS have reiterated the necessity for data security and privacy concerning health information.

30. The FTC published a bulletin entitled *Protecting the privacy of health information: A baker’s dozen takeaways from FTC cases*, in which it noted that “[h]ealth information is not just about medications, procedures, and diagnoses. Rather, it is anything that conveys information—or enables an inference—about a consumer’s health. Indeed, [recent FTC enforcement actions involving] Premom, BetterHelp, GoodRx and Flo Health make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for

example—or how they interact with that app (say, turning ‘pregnancy mode’ on or off) may itself be health information.”⁸

31. The FTC informs companies that provide healthcare services that they should not use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

Don’t use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers. In today’s surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. But when companies use consumers’ sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out. [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers’ affirmative express consent for the disclosure of sensitive health information.⁹

32. HHS affirmed that HIPAA and its regulations prohibit the transmission of individually identifiable health information (“IIHI”) by tracking technology like the Google and Meta without the patient’s authorization and other protections like a business associate agreement with the recipient of patient data.¹⁰

⁸ See Elisa Jillison, *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases*, the FTC Business Blog (July 25, 2023), <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases>.

⁹ *Id.* (emphasis added).

¹⁰ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (noting that “IIHI collected on a regulated entity’s website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.”). This guidance was recently vacated in part due to the court finding it in part to be the product of improper rulemaking,

33. In July 2023, the FTC and HHS sent a letter to approximately 130 healthcare providers warning them about the use of online tracking technologies that could result in unauthorized disclosures of PHI to third parties.¹¹ The letter highlighted the “risks and concerns about the use of technologies, such as the Meta/Facebook Pixel and Google Analytics, that can track a user’s online activities,” and warned about “[i]mpermissible disclosures of an individual’s personal health information to third parties” that could “result in a wide range of harms to an individual or others.”¹² According to the letter, “[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more.”¹³

34. Despite these clear warnings from federal regulators, Defendant Beaumont embedded Tracking Tools on its Website to secretly track its patients’ communications regarding

and it is cited for reference only until OCR updates its guidance, should it do so in the future. *See American Hosp. Ass’n. v. Becerra*, 2024 WL 3075865 (S.D. Tex., Jun. 20, 2024). The Court’s Order found only that OCR’s guidance regarding covered entities’ collection and disclosure to third parties of users’ IP addresses while they navigated unauthenticated public webpages (“UPWs”) was improper rulemaking. The Order in no way affects or undermines OCR’s guidance regarding covered entities disclosing unique personal identifiers, such as Google or Facebook identifiers, to third parties while patients make appointments for particular conditions, pay medical bills or log into (or use) a patient portal. *See id.* at 3-4, 31, n. 8 (vacating OCR guidance with respect to the “Proscribed Combination” defined as “circumstances where an online technology connects (1) an individual’s IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers” but stating that “[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document.”).

¹¹ <https://www.ftc.gov/business-guidance/blog/2023/07/ftc-hhs-joint-letter-gets-heart-risks-tracking-technologies-pose-personal-health-information>

¹² https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

¹³ *Id.*

healthcare information and disclose those communications to third parties.

B. The Meta Pixel

35. Through its Web Properties, Defendant connects Plaintiff and Class Members to Defendant's digital health care platforms with a core goal of increasing profitability.

36. In furtherance of that goal, and to increase the success of its advertising and marketing, Defendant purposely embedded and deployed the Meta Pixel on its Website and, upon information and good faith belief, its Portal. By doing so, Defendant surreptitiously shared its patients' and prospective patients' identities and online activity including private communications and search results related to conditions, symptoms, treatments, and physicians with Meta.

37. Meta's core business function is to sell advertising, and it does so on several platforms, including Facebook and Instagram. The bulk of Meta's billions of dollars in annual revenue comes from advertising—a practice in which Meta actively participates by using algorithms that approve and deny ads based on the ads' content, human moderators that further review ads for both legality and aesthetics prior to and after the ads are published, and other algorithms that connect ads to specific users, without the assistance or input of the advertiser.

38. Over the last decade, Meta has become one of the largest and fastest growing online advertisers in the world. Since its creation in 2004, Facebook's daily, monthly, and annual user base has grown exponentially to billions of users.

39. Meta's advertising business has been successful due, in significant part, to Meta's ability to target users, both based on information users provide to Meta, and based on other information about users Meta extracts from the Internet at large. Given the highly specific data used to target particular users, thousands of companies and individuals utilize Facebook's advertising services.

40. One of Meta's most powerful advertising tools is the Meta Pixel, which it first launched as the Facebook Pixel in 2015.

41. The Pixel was branded as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website." Meta stated:

Facebook pixel, [is] a new way to report and optimize for conversions, build audiences[,] and get rich insights about how people use your website. We're also announcing the availability of custom conversions, a new rule-based method to track and report conversions for your Facebook ads.

Facebook pixel makes things simple for advertisers by combining the functionality of the Conversion Tracking pixels and Custom Audience pixels into a single pixel. You only need to place a single pixel across your entire website to report and optimize for conversions. Since it is built on top of the upgraded Custom Audience pixel, all the features announced in our previous blog post (Announcing Upgrades to Conversion Tracking and Optimization at Facebook) are supported through Facebook pixel as well.

[Advertisers and website operators] can use Facebook pixel to track and optimize for conversions by adding standard events (e.g., Purchase) to your Facebook pixel base code on appropriate pages (e.g., purchase confirmation page).¹⁴

42. The Pixel is an easily attainable piece of code that Meta makes available to website developers for free. In exchange, at a minimum, website developers must agree to Meta's Business Tool Terms.¹⁵

43. The Business Tools Terms note that the Meta's Business Tools including the Pixel capture two types of information: "Contact Information" which "personally identifies individuals,"

¹⁴ Cecile Ho, *Announcing Facebook Pixel*, Meta (Oct. 14, 2015), <https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/>.

¹⁵ See [Meta Business Tool Terms](https://www.facebook.com/legal/businesstech?paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zui0STn-VURAyVhvIzw1Df5nxIgiuXOqcd5A8yKuEtk&_rdr), https://www.facebook.com/legal/businesstech?paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zui0STn-VURAyVhvIzw1Df5nxIgiuXOqcd5A8yKuEtk&_rdr ("When you use any of the Meta Business Tools . . . or otherwise enable the collection of Business Tool Data . . . these Business Tool Terms govern the use of that data").

and “Event Data” which contains additional information about people and their use of a developer’s website.¹⁶

44. The Business Tools Terms also require websites to “provide[] robust and sufficiently prominent notice to users . . . on each web page where our pixels are used that links to a clear explanation (a) that third parties, including Meta, may . . . collect or receive information from your websites and elsewhere on the Internet and use that information to . . . deliver ads, (b) how users can opt out of the collection and use of information . . . and (c) where a user can access a mechanism for exercising such choice[.]”¹⁷

45. Even with these protocols in place, Meta prohibits the disclosure of Business Tools Data “that you know or reasonably should know . . . includes health, financial information or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines).”¹⁸

46. After agreeing to the Business Tools Terms, website developers can choose to install and use the Pixel on their websites to track and measure certain actions, such as a website visitor’s text searches and page views, including the detailed URLs triggered by page views. When a website visitor takes an action a developer chooses to track on its website, the Pixel is triggered and sends data about that “Event” to Meta. All of this happens without the user’s knowledge or consent.

47. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each “client

¹⁶ *Id.*, § 1(a)(i)-(ii).

¹⁷ *Id.*, § 3(c)(i).

¹⁸ *Id.*, § 1(h).

device” (such as a computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google’s Chrome browser, Mozilla’s Firefox browser, Apple’s Safari browser, and Microsoft’s Edge browser).

48. Every website is hosted by a computer “server” that holds the website’s contents and through which the entity in charge of the website exchanges communications with Internet users’ client devices via their web browsers.

49. A browsing session online may consist of thousands of web communications. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- An **HTTP Request** is an electronic communication a website visitor sends from his device’s browser to the website’s server. There are two types of HTTP Requests: (1) GET Requests, which are one of the most common types of HTTP Requests—in addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies; and (2) POST Requests which can send a large amount of data outside of the URL. In this case, a patient’s HTTP Request would be asking Defendant’s Website to get certain information, such as a list of clinic locations or prescriptions. So that servers can better understand what information users are requesting, HTTP Requests also use URLs that contain parameters, which use variables and assigned values in the URL to pass additional information through the HTTP Request.
- **Cookies** are a text file that website operators and others use to store information on the website visitor’s device; these can later be communicated to a server or servers. Cookies are sent with HTTP Requests from website visitor’s devices to the host server. Some cookies are “third-party cookies,” which means they can store and communicate data when visiting one website to an entirely different website. Third-party cookies are created by a website with a domain name other than the one the user is visiting, in this case Meta.¹⁹ There are also “first-party cookies,” like the fbp

¹⁹ *Third-Party Cookie*, <https://www.pcmag.com/encyclopedia/term/third-party-cookie>. This is also confirmable using web developer tools to inspect a website’s cookies and track network activity.

cookie, which is created by the website the user is visiting, in this case Defendant.²⁰ Meta uses both first- and third-party cookies in Pixel to link Facebook IDs and Facebook profiles, and Defendant sends these identifiers to Meta.

- An **HTTP Response** is a response to an HTTP Request. It is an electronic communication that is sent as a reply to the website visitor's device's web browser from the host server. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data. The HTTP Response is when the website sends the requested information (*see* the HTTP Request); this is sometimes called the "Markup."

50. A user's HTTP Request asks Defendant's Website to retrieve certain information (such as "Orthopedics"). The HTTP Response then renders or loads the requested information in the form of Markup (i.e., the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website).

51. Every website, including Defendant's, is composed of Markup and "Source Code."

52. Source code is a set of instructions that commands the website visitor's browser to take certain actions when the web page loads or when a specified event triggers the code.

53. Source code may also command a web browser to transmit data to third parties in the form of an HTTP Request. Such data transmissions allow a website to export data about users and their actions to third parties. Third parties receiving this data are typically configured to track user data and communications for marketing purposes.

54. Transmission of such data occurs in the background without notifying the web browser's user. The pixels are invisible to website users and thus, without any knowledge, authorization, or action by the user, the website site developer (or website commander) can use its source code to contemporaneously and invisibly re-direct the user's PII and PHI to third parties. Through the Pixel, Defendant uses source code that can accomplish just that.

²⁰ *First-Party Cookie*, <https://www.pc当地.com/encyclopedia/term/first-party-cookie>. This is confirmable using web developer tools to inspect a website's cookies and track network activity.

55. The Pixel “tracks the people and the types of actions they take.”²¹ According to Meta, the Pixel is a piece of code that allows Defendant to measure the effectiveness of [its] advertising by understanding the actions [website visitors] take on [its] website.”²² Thus, by secretly recording and transmitting data to Meta—without the user’s knowledge or consent—the Pixel acts much like a traditional wiretap controlled by Defendant.

56. Through this online tracking technology, Meta intercepts each page a user visits, what buttons they click, as well as the specific information the user inputs into the website and other searches conducted. The Pixel sends each of these pieces of information to Meta with PII, such as the user’s IP address. Meta stores this data on its own servers, in some instances for years on end, and independently uses the data for its own financial gain.

57. This data is then associated with the individual user’s Facebook account. For example, if the user is logged into their Facebook account (or has been logged in recently) when the user visits Defendant’s website, Meta receives several cookies allowing Meta to link the data collected by the Pixel to the specific Facebook user. In other words, a user’s personal and private information sent by the Meta Pixel to Facebook is sent alongside that user’s personal identifiers, including IP address and unique cookie values, which can be linked to the user’s unique Facebook account.

58. Meta accomplishes this by placing cookies in the web browsers of users logged into their services, which aids Meta in identifying users.

59. One such example is the “c_user” cookie, which is a third-party cookie assigned to

²¹ *Retargeting*, Facebook, <https://www.facebook.com/business/goals/retargeting>.

²² *About Meta Pixel*, Meta Business Help Center, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

each person with a Facebook account. The “c_user” cookie contains a numerical value known as the Facebook ID that uniquely identifies a Facebook user. It is composed of a unique and persistent set of numbers.

60. A user’s Facebook ID is linked to their Facebook profile, which contains a wide range of demographic and other information about the user including pictures, personal interests, work history, relationship status, and other details.

61. Because a user’s Facebook ID uniquely identifies their Facebook account, Meta—or any ordinary person—can use the Facebook ID to locate, access, and view the user’s corresponding Facebook profile. Thus, when a Facebook user visits Defendant’s Website while logged in to their Facebook account, the Pixel transmits the user’s private web communications with Defendant along with the “c_user” cookie. Meta can then use this information to match the web communications with the user’s Facebook ID.

62. Even if a user does not have a Facebook account or is not logged in to Facebook when browsing Defendant’s Website, the Pixel transmits the user’s web communications with Defendant’s Website to Meta along with a unique identifier associated with another cookie called the “_fbp” cookie, which is transmitted as first-party cookie. Meta can then use that unique identifier to link the user’s web communications with the user’s Facebook ID. And if a user who does not have a Facebook account later creates an account, Meta may be able to associate the user’s historical browsing history intercepted via the Pixel and “_fbp” cookie to the newly created account.

63. Meta’s Business Tools Terms make clear that the Pixel is meant to “match the Contact Information” of users “against user IDs . . . as well as to combine those user IDs with

corresponding Event Data.”²³

64. After Meta processes users’ intercepted information, it makes the relevant analytics available to Beaumont through Meta’s Event Manager tool.

65. Using the Events Manager, Beaumont can review a summary of users’ activity including the pages, parameters, and URLs sent through the Pixel,²⁴ as well as any included metadata.²⁵

66. Without any knowledge, authorization, or action by a user, a website owner like Defendant can use its Source Code to commandeer the user’s computing device, causing the device to contemporaneously and invisibly re-direct the users’ communications to Meta. Meta then uses this information to match the user with their Facebook ID.

67. Judge William H. Orrick on the United States District Court for the Northern District of California summarized how this process plays out:

To understand how the Meta Pixel typically works, imagine the following scenario. A shoe company wishes to gather certain information on customers and potential customers who visit its website. The shoe company first agrees to Meta’s Business Tools Terms (discussed below), which govern the use of data from the Pixel. The shoe company then customizes the Meta Pixel to track, say, every time a site visitor clicks on the “sale” button on its website, which is called an “Event.” Every time a user accesses the website and clicks on the “sale” button (i.e., an “Event” occurs),

²³ *Meta Business Tool Terms*, Section 2(a)(i)(1), https://www.facebook.com/legal/businesstech?paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zui0STn-VURAyVhvIzw1Df5nxIgiuXOqcd5A8yKuEtk&_rdr.

²⁴ *How to view pages, parameters and URLs in Meta Events Manager*, <https://www.facebook.com/business/help/815029860145251> (“In Meta Events Manager, you can see a summary of pages, parameters and URLs recently sent through the Meta Pixel . . .”).

²⁵ A web developer using the Events Manager can “[c]lick on the filter icon to select what activity types and details are display.” Developers can sort by activity types, including “automatically logged pixel events,” which may contain metadata. *Test your app or web browser events using the test events tool*, <https://www.facebook.com/business/help/2040882565969969?id=1205376682832142>.

it triggers the Meta Pixel, which then sends certain data to Meta. Meta will attempt to match the customer data that it receives to Meta users—Meta cannot match non-Meta users. The shoe company may then choose to create “Custom Audiences” (i.e., all of the customers and potential customers who clicked on the “sale” button) who will receive targeted ads on Facebook, Instagram, and publishers within Meta’s Audience Network. Meta may also provide the shoe company with de-identified, aggregated information so the shoe company understands the impact of its ads by measuring what happens when people see them. Meta does not reveal the identity of the matched Meta users to the shoe company.²⁶

68. The Pixel also allows a healthcare company, like Defendant, to impact the delivery of ads, measure cross-device conversions, create custom audiences, and save money on advertising and marketing costs.²⁷ But, most relevant here, the Pixel allowed Defendant and Meta to track users secretly on Defendant’s Web Properties and intercept their communications with Defendant.

69. When visitors to Defendant’s Web Properties, like Plaintiff and Class Members, communicated with Defendant or inquired about personal health-related topics, that information was transmitted to and intercepted by Meta.

70. The PHI intercepted, recorded, and transmitted to Meta includes, but is not limited to, exact search terms and search results, patient status, health symptoms, health conditions, treatments, appointment details, and physicians and locations sought.

71. During that same transmission, Defendant would also provide Meta with the patient’s PII, such as their Facebook ID number, persistent cookies, device ID, and computer IP addresses. This information makes it easy to link private communications with Defendant via the

²⁶ *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at *2 (N.D. Cal. Dec. 22, 2022) (internal citations omitted). In describing Pixel technology in *In re Meta Pixel Healthcare Litigation*, the court referenced the declaration of expert Richard M. Smith, which details the manner in which the challenged Pixel technology works and Meta’s arrangements with health providers that employ it. See Declaration of Richard M. Smith, *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO (N.D. Cal.) [ECF 49].

²⁷ *Meta Pixel*, https://www.facebook.com/business/tools/meta-pixel?ref=search_new_2.

Web Properties to a specific and identifiable Facebook user.

72. Once Meta has that data, it processes, analyzes, and assimilates it into databases like Core Audiences or Custom Audiences for advertising purposes. If the website visitor is also a Facebook user, Meta will associate the information that it collects from the visitor with a Facebook ID that identifies the user's name and Facebook profile.

73. In sum, the Pixel allows Meta to learn, manipulate, and use for financial gain, the medical and private content Defendant's Web Properties visitors communicated, viewed, or otherwise interacted with on Defendant's Web Properties.

C. Google Tracking Code.

74. Like the Meta Pixel, Google creates code that website developers can install on their websites to track user activity. Whenever a user visits a website that is running Google tracking code, Google's code directs the user's browser to send a separate and concurrent communication to Google without the user's knowledge.

75. The information that is intercepted and transmitted to Google via the Google tracking code includes: (i) the URL of the specific webpage a user is trying to access; (ii) the user's IP address; (iii) the User-agent, which identifies the user's device platform and browser; (iv) the user's geolocation, if available; (v) the Referer, which is the URL of the page on which the user clicked a link to access a new page; (vi) event data, which describes how users interact with a website, for example, whether they looked up a provider or made an appointment; and (vii) actual search queries on the site.

76. Google tracking code tells Google exactly what a user's browser communicated to the website.

77. Like with the Meta Pixel, the user's communications to the website are transmitted

to Google together with cookies and other unique identifiers that Google can use to match the communications to individuals who use Google's services.

78. Information sent to Google is sent alongside the users' unique identifiers (including DSID and IDE cookies from DoubleClick), thereby allowing individual patients' communications with Beaumont, and the PHI and PII contained in those communications, to be linked to their unique Google accounts and therefore their identity.²⁸

79. Similar to the way that Facebook's _fbp cookie operates, Google Analytics also uses certain "first-party" cookies like _ga and _gid (unique to each specific website) to track users' activities on non-Google websites.

80. Google logs a user's browsing activities on non-Google websites and uses this data for serving personalized ads.

D. Beaumont Deploys Third-Party Tracking Tools to Intercept and Disclose PHI and PII.

81. As an example of how the Meta Pixel operated on Beaumont's Website, consider a visitor who goes to the Website and uses the search bar to search for "cancer."

82. The search result takes the visitor to the <https://www.beaumont.org/search-results?cancer> webpage. When doing so, the visitor's browser sends a GET Request to Defendant's server, requesting that server to load the webpage.

83. At the same time, the Pixel causes the visitor's browser to secretly intercept and record the visitor's communication with Beaumont's Website including the specific URL

²⁸ See *Brown v. Google LLC*, 2023 WL 5029899, at fn. 6, note 5, *supra* (quoting Google employee deposition testimony explaining how Google tracks user data). Upon information and belief, Google uses DoubleClick cookies such as DSID and IDE that operate similarly to the unique Facebook ID, to track users across websites and target them with ads based on their browsing activities.

requested and transmit the private communication to Meta with unique identifiers used to link the communication to a specific Facebook user, as shown in *Figure 1*:

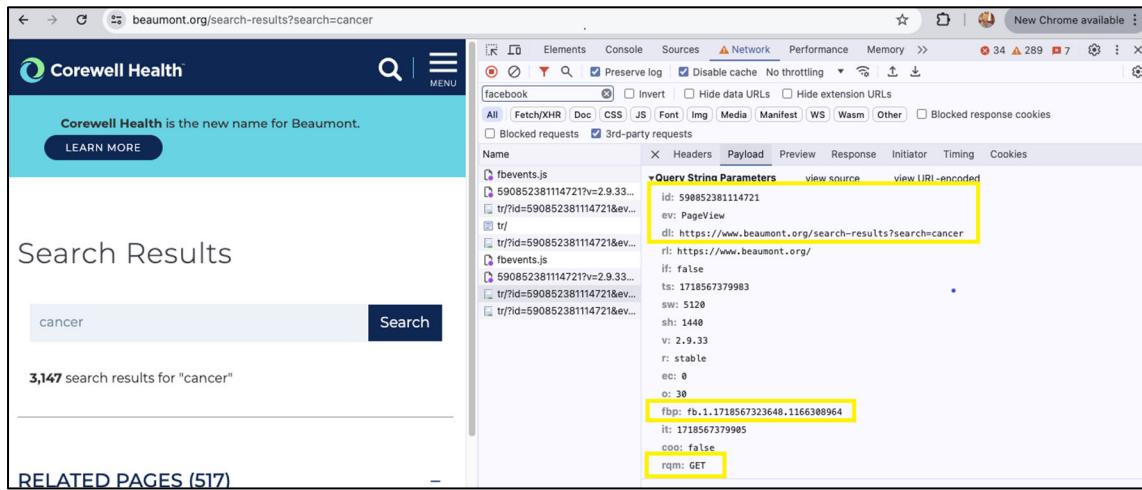


Figure 1: Depiction of user's search information for "cancer" intercepted and recorded by the Facebook Pixel to Meta via a "PageView" event.

84. As reflected in *Figure 1*, the “dl” path shows the specific URL for the page requested by the visitor’s browser, including the substantive description and disclosure of the visitor’s search for “cancer.” This transmission, as explained herein, also contains the Pixel’s transmission of the `_fbp` cookie, the `c_user` cookie (the Facebook ID), and other cookies and identifiers used to identify the website visitor by name and Facebook account. Thus, the fact that a patient or prospective patient is using or considering using Beaumont for healthcare services related to cancer is transmitted to Meta. Disclosure of that information reveals to Meta the website visitor’s status as a patient or prospective patient with Beaumont, seeking services or treatment for cancer.

85. The first line of Source code text, “`id: 590852381114721`” refers to Beaumont’s Pixel ID and confirms that Defendant has downloaded the Facebook Pixel into their Source Code for this webpage.

86. The second line of text, “`ev: PageView,`” identifies and categorizes which actions

the user took on the webpage (“ev=” is an abbreviation for event, and “PageView” is the type of event). Thus, this identifies the user as viewing the page with search results for their “cancer” query to Beaumont.

87. If that same patient inquired about specific cancer treatment center or a provider specializing in cancer, the Pixel would likewise intercept those communications and transmit them to Meta along with the patient’s unique identifiers, as reflected in *Figures 2-3* below.

The screenshot shows a list of request headers for a network request. Several fields have been highlighted with yellow boxes:

- :authority:** www.facebook.com
- :method:** GET
- :path:** /tr? id=590852381114721&ev=Microdata&dl=https%3A%2F%2Fdoctors.beaumont.org%2Fsearch%3FUnified%3FOncology%26sort%3Dnetwork%252Crelevance%26tt%3D11aafd10-812e-486c-9914-b3b855283885%26ut%3D661674e4-968b-4c49-a2f6-d8df5eef9647%26timestamp%3D2024-06-16T19%253A55%253A33.420Z&rl=https%3A%2Fwww.beaumont.org%2Fservices%2Fdoctors&if=false&ts=1718567737001&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Oncology%20-%22%20Find%20a%20Doctor%20%7C%20Beaumont%20Health%22%2C%22meta%3Adescription%22%3A%22Oncology%20-%20Nationally%20recognized%2C%20Beaumont%20Health%20has%20nearly%205%20000%20doctors%20throughout%20the%20Metro%20Detroit%20area.%20Find%20a%20Beaumont%20specialist%20near%20you.%22%7D&cd[OpenGraph]=%7B%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=5120&sh=1440&v=2.9.33&r=stable&ec=1&o=30&bp=fb.1.1718567323648.1166308964&it=1718567735435&coo=false&es=automatic&tm=3&rqm=GET
- :scheme:**
- Accept:** image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
- Accept-Encoding:** gzip, deflate, br, zstd
- Accept-Language:** en-US,en;q=0.9
- Cache-Control:** no-cache
- Cookie:** sh-1FFa7e65ACM IN7V/hw IOIOEah; datr=1EFeZpNGkA0lyVv1A5baMIOfc_c_user=100 [REDACTED]22; dpr=1; xs=20%3ARFkwEny8X245DQ%3A2%3A1717453271%3A-1%3A-1%3A%3AaclI-U_iGsk-AnnG_ln9nPcFvAskN2eGHv9zCilJnFdA; fr=15tdGCra7w8ZdqE7Y.AWWkZDPP-10Yg4qz57x0Wy0rQas.BmaGWL..AAA.0.0.BmaGWL.AWVYsNTTdho
- Pragma:** no-cache
- Priority:** i
- Referer:** https://doctors.beaumont.org/
- Sec-Ch-Ua:** "Google Chrome";v="125", "Chromium";v="125"

Figure 2: Depiction of a patient’s search for an Oncology provider on Beaumont’s Website being captured and disclosed by the Facebook Pixel to Meta along with the user’s PII (including the c_user, datr and fr cookies), via a ‘Microdata’ event

The screenshot shows a search result for "Oncology" on the Corewell Health website. The search bar contains "Oncology". Below it, a list of 197 providers is shown, with the first provider being "Shanti Thomas, MD". The provider's profile includes a photo, specialties (Medical Oncology, Hematology), and a rating of 4.8 out of 5 based on 960 reviews. A "Request Appointment" button is visible. The browser's Network tab is open, showing the request parameters for the appointment booking. The URL is https://doctors.beaumont.org/search?unified=Oncology&sort=networks%2Crelevance&tt=11aaf10-812e-486c-9914-b3b855283885&ut=661674... The parameters include id: 590852381114721, ev: MicroEvent, and fb: fb.1.1718567323648.1166308964.

Figure 3: An easier to read depiction of a patient’s search for in-person care from an oncologist.

88. The Website provides an option for patients to make an appointment with a specialist. If the patient or prospective patient clicked the “Request Appointment” button, Beaumont’s Pixel also intercepted those communications, including the provider’s specialty, and transmitted them to Meta together with the patient’s unique identifiers:

The screenshot shows a modal window titled "Book an Appointment with Shanti Thomas, MD". Inside the modal, there is a "Contact Us" section with a phone icon and the number "Call 734-479-2371". Below the modal, the main search results for "Shanti Thomas, MD" are displayed, showing her photo, specialties (Medical Oncology, Hematology), a rating of 4.8 out of 5 based on 960 reviews, and a "Request Appointment" button. The browser's Network tab is open, showing the request parameters for the appointment booking. The URL is https://doctors.beaumont.org/search?unified=Oncology&sort=networks%2Crelevance&tt=11aaf10-812e-486c-9914-b3b855283885&ut=661674... The parameters include id: 590852381114721, ev: SubscribedButtonClick, and fb: fb.1.1718567323648.1166308964.

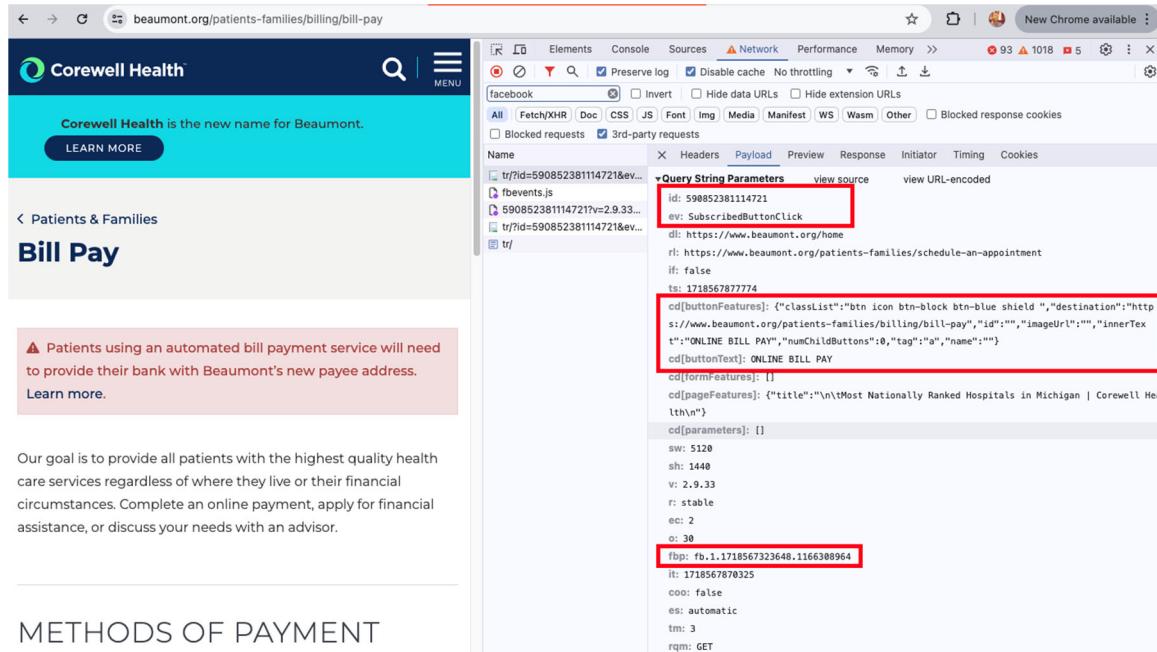
Figure 4: Depiction of a SubscribedButtonClick “event” disclosing that the patient is attempting to make an appointment with an oncologist, along with the Facebook _fbp cookie.

89. Further, Beaumont’s Website captured disclosed patients’ communications as they logged into and signed up for the patient portal, and patients’ bill pay activities, see **Figures 6-7** below:

```

▼ Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr?_
id=5908523811147218ev=SubscribedButtonClick&dl=https%3A%2F%
2Fwww.beaumont.org%2Fhome&rl=https%3A%2F%2Fwww.beaumont
.org%2Fpatients-families%2Fschedule-an-
appointment&if=false&ts=171856787774&cd[buttonFeatures]=%7B
%22classList%22%3A%22btn%20icon%20btn-block%20btn-
blue%20shield%20%22%2C%22destination%22%3A%22https%3A%
2F%2Fwww.beaumont.org%2Fpatients-families%2Fbilling%2Fbill-
pay%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22
%22%2C%22innerText%22%3A%22ONLINE%20BILL%20PAY%22%2
C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C
%22name%22%3A%22%22%7D&cd[buttonText]=ONLINE%20BILL%2
0PAY&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%2
2%3A%22%5Cn%5CtMost%20Nationally%20Ranked%20Hospitals
%20in%20Michigan%20%7C%20Corewell%20Health%5Cn%22%7D&
cd[parameters]=%5B%5D&sw=5120&sh=1440&v=2.9.33&r=stable&
c=2&o=30&fbp=fb.1.1718567323648.1166308964&it=171856787032
5&coo=false&es=automatic&tm=3&rqm=GET
:scheme: https
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*/*;q=0.8
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Cache-Control: no-cache
Cookie: sb=1EFeZs65ACMJNZVhwJOIOEah;
datr=1EFeZpNGka0lyVv1A5baMIOfc_user=10 [REDACTED];22;
dpr=1; xs=20%3ARFkwEny8X245DQ%3A2%3A1717453271%3A-
1%3A-1%3A%3AAcU-u_iGsk-AnpG_lp9qPcEyASkN2eGHv9zCiUqFdA;
fr=15tdGCra7w8ZdqE7Y.AWWkZDPP-
I0Yg4qz57x0Wy0rQas.BmaGWL..AAA.0.0.BmaGWL.AWVYsNTTdho
Pragma: no-cache
Priority: i
Referer: https://www.beaumont.org/home

```



Figures 6-7: Depiction of Defendant capturing and disclosing patient's bill payment activities, with PHI and PII (including the c_user, datr, fr and the _fbp cookies) disclosed by Beaumont's Meta Pixel via a 'SubscribedButtonClick' event.

90. In each of the examples above, the user's website activity and the contents of the user's communications are sent to Facebook alongside their personally identifiable information. Several different methods allow marketers and third-parties to identify individual website users, but the examples above demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Pixel. For example, the Pixel transmits the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

91. Facebook receives several cookies when Beaumont's Website transmits information via the Pixel, including the c_user, datr, and fr cookies, as evidenced by the images *supra*.

92. The "datr" cookie contains a unique alphanumeric code and identifies the specific

web browser from which the user is sending the communication. It is an identifier that is unique to the user's web browser and is therefore a means of identification for Meta. Meta keeps a record of every datr cookie identifier associated with each of its users.

93. The fr cookie, a unique combination of the c_user and datr cookies, contains an encrypted Facebook ID and browser identifier.²⁹ Facebook, at a minimum, uses the fr cookie to identify users, and this particular cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.³⁰

94. The datr and fr cookies are commonly referred to as third-party cookies because they were "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. Although Facebook created these cookies, Defendant is ultimately responsible for the manner in which individual website users were identified via these cookies, and Facebook would not have received this data but for Defendant's implementation and use of the Pixel throughout the Beaumont Website.

95. Defendant also revealed the Website visitors' identities via first-party cookies such as the _fbp cookie that Facebook uses to identify a particular browser and a user, *see Figure 8:*



```

cd[buttonText]: Request Appointment
cd[formFeatures]: []
cd[pageFeatures]: {"title":"Oncology - Find a Doctor | Beaumont Health"}
cd[parameters]: []
sw: 5120
sh: 1440
v: 2.9.33
r: stable
ec: 2
o: 30
fbp: fb.1.1718567323648.1166308964
it: 1718567735435

```

²⁹ Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit*, p. 33 (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited Oct. 25, 2024).

³⁰ *Cookies & other storage technologies*, <https://www.facebook.com/policy/cookies/> (last visited Oct. 25, 2024).

96. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Beaumont's use of the Facebook Meta Pixel program. The fbp cookie emanates from Defendant's Website as a putative first party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy. Therefore, the _fbp cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies.

97. Google Analytics also uses "first-party" cookies like _ga and _gid (unique to each specific website) to track users' activities on non-Google websites.

98. The __ga and __gid cookies communicate users' information to Google similarly to the way that Facebook's _fbp cookie operates.

99. The Facebook Pixel uses both first- and third-party cookies to link website visitors' communications and online activity with their corresponding Facebook profiles, and, because the Pixel is automatically programmed to transmit data via both first-party and third-party cookies, customers' information and identities are revealed to Facebook even when they have disabled third-party cookies within their web browsers.

100. At present, the full breadth of Beaumont's tracking and data sharing practices is unclear, but other evidence suggests Defendant has been using additional Tracking Tools to transmit its patients' PHI to additional third parties. For example, Plaintiff's counsels' investigation revealed that Defendant is also sending their patients' protected health information to Google via Google tracking tools including Google Analytics and Google Tag Manager.

101. Google Tracking Tools installed on the Beaumont Website appear to collect the same types and categories of sensitive PHI from Defendant's patients as the Facebook

Pixel.

102. In addition, Google trackers disclose patient portal activities to Google, such as when a patient visits the MyBeaumontChart login page, via ‘pageview’ and DoubleClick events:

The screenshot shows a web browser window with the URL https://mybeaumontchart.com/mychart/Authentication/Login?_gl=1*1wijnv3*_gcl_au*MTA1MjQ1NTA2MC4xNzE4NTYzNjk1*_ga*MTk0NTkyNjAyOC.... The page is the Corewell Health Beaumont patient portal login screen. On the right, the browser's developer tools Network tab is open, showing several 'collect' requests. Some specific headers are highlighted with red boxes:

- :authority:** stats.g.doubleclick.net
- :method:** POST
- :path:** //collect?t=dc&aip=1&r=3&v=101&a=785...
- :scheme:** https
- Accept:** */*
- Accept-Encoding:** gzip, deflate, br, zstd
- Accept-Language:** en-US,en;q=0.9
- Cache-Control:** no-cache
- Content-Length:** 0
- Content-Type:** text/plain
- Cookie:** ar_debug=1; DSID=AJSUUb0oStd8568dfh0brarf4nJpp5qM7iq9Xa3KlynI9WoA0TMcA2eufdkUa722R3UXBwdF8vmF_cqRtWGBNevdrd8wYZxmQh9VaejR4PcltzifKrezbC6CChlUhK9-yxjQ0RmrRaH02JED1-30HjGMyFk-hiyXuVWL-TlLqFRKwyrruk4allSLK-CnypqAvS3xJgsd_rfon700arX25zHy5veeMeO8HhKWwOT1hpkMGQz8rrfZnRz9l8ISYOG4Hm0GajrnEqSNys6zt3uPpmrh9IA6y2NSKoV7yvI0h2sengc; IDE=AHwqTUJchbBw9zAbabcTU49bNQsHlgUWaqlVHzXpZ5DEvMlkq5EHVE_SEBS7/g37qi
- Origin:** https://mybeaumontchart.com
- Pragma:** no-cache
- Priority:** u=1, i
- Referer:** https://mybeaumontchart.com/
- Sec-Ch-Ua:** "Google Chrome";v="125", "Chromium";v="125",

The screenshot shows a web browser window for myBeaumontChart.com. On the left, there is a login form with fields for 'myBeaumontChart Username' and 'Password', and a 'Sign in' button. Below the form are links for 'Forgot username?' and 'Forgot password?'. To the right of the form, a 'New User Sign up' button is visible. At the bottom of the page, there are links for 'Pay Bill Online', 'Resources and Tools', and 'Frequently Asked Questions'. On the far right, the browser's developer tools are open, specifically the Network tab. A red box highlights the URL in the 'Headers' section: 'https://mybeaumontchart.com/mychart/Authentication/Login?_gl=1*1wijnv3*_gcl_au*MTA1MjQ1NTA2MC4xNzE4NTYzNjk1*_ga*MTk0NTkyNjAyOC...'. Another red box highlights the value of the '_gid' cookie in the 'Payload' section: '498991112.1718569383'.

Figures 9-10: Example of Beaumont’s Website sending information to Google that a patient is attempting to access their patient portal account.

103. As described *supra*, this information is shared with Google along with the DSID, IDE, __ga and __gid cookies.

104. Based on the above examples of how the Tracking Tools operate on Beaumont’s Website, Meta and Google would know (i) that a particular individual—who Meta and Google could identify based on their respective accounts—was a patient or prospective patient of Beaumont seeking healthcare services, (ii) that the named patient searched for information regarding their specific medical condition (for example, cancer), and (iii) that the patient in question was attempting to make an appointment with specific physicians, pay their bill, or log into their patient portal.

105. Meta and Google would also know the named patient’s location and IP address, among other identifiers associated with the patient’s computer or cell phone.

106. Using this PHI and PII, technology companies can put the named patient into a

Core or Custom Audience for purposes of targeted advertising by Beaumont or any other company seeking to advertise its services or products to individuals that fit the named patient's profile.

107. Beaumont, Meta, Google, and other third parties profit off of Plaintiff's and Class Members' PHI and PII without their knowledge, consent, or authorization.

108. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (a) embedded and implemented the Tracking Tools, which surreptitiously intercepted, recorded, and disclosed Plaintiff's and other online patients' and prospective patients' confidential communications and private medical information; (b) disclosed patients' and prospective patients' protected information to Meta and Google—unauthorized third parties; and (c) failed to provide notice to or obtain the consent from Plaintiff and Class Members to share their PHI and PII with others.

E. Plaintiff's Representative Experiences.

Plaintiff Fateen

109. Plaintiff Fateen accessed and used the Beaumont Website through her computer and mobile devices while located in Michigan to seek medical treatment as recently as July 2024.

110. Plaintiff Fateen has been a patient of Beaumont since approximately 2020.

111. Plaintiff Fateen began using Defendant's Web Properties in 2020 or earlier to, among other things, search for specialty providers including a dermatologist in or around January 2023, search for Beaumont locations, pay for medical services, schedule appointments, use the Patient Portal, and search for information regarding treatments and conditions for medical conditions.

112. Information that Plaintiff Fateen provided to Defendant via its Website included queries about her medical conditions as well as for specialty doctors.

113. Plaintiff Fateen had an active Facebook account and an active Google account during the time she was providing her PHI and PII to Defendant via its Website.

114. After she provided information to Defendant regarding her PHI and PII, Plaintiff Fateen began receiving advertisements on her Facebook account for Beaumont treatments and services, including various trials.

115. Plaintiff Fateen reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by any third party without her full knowledge and informed consent.

116. Plaintiff Fateen provided her PHI and PII to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

117. As described herein, Defendant worked along with Facebook to intercept Plaintiff Fateen communications, including those that contained confidential PHI and PII, while Plaintiff Fateen was within the state of Michigan.

118. Defendant willfully facilitated these interceptions without Plaintiff Fateen' knowledge, consent or express written authorization.

119. Within the State of Michigan, Defendant transmitted Plaintiff Fateen' FID, unique Google identifiers, computer IP address, location, information such as medical treatments and conditions, the information on physician(s) she selected and her sensitive and private medical information to Facebook and Google.

120. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to third party data brokers can only be determined through formal discovery. However, Defendant intercepted at least communications about Plaintiff's past or present patient

status, medical conditions, treatments sought including dermatological care, and the locations for receipt of healthcare, via descriptive long-URLs, microdata and the inner text of buttons clicked by Plaintiff on the Website, that were sent to Meta via the Pixel and which contained information concerning Plaintiff's specific medical conditions, queries, and treatments sought.

121. By doing so without her consent, Defendant breached Plaintiff Fateen' right to privacy and unlawfully disclosed her PHI and PII.

122. Defendant did not inform Plaintiff Fateen that it shared her PHI and PII with Facebook.

123. Plaintiff Fateen suffered damages in, inter alia, the form of (i) invasion of privacy; (ii) violation of confidentiality of her PHI and PII; (iii) loss of benefit of the bargain; (iv) diminution of value of the PHI and PII; (v) statutory damages and (vi) the continued and ongoing risk to her PHI and PII.

124. Plaintiff Fateen has a continuing interest in ensuring that her PHI and PII is protected and safeguarded from future unauthorized disclosure. Plaintiff Fateen wants to continue to communicate through online platforms but has no practical way of knowing if her communications are being intercepted and disclosed to Facebook and/or Google, and thus continues to be at risk of harm from Defendant's conduct.

F. Beaumont's Conduct Violates Its Own Privacy Policies and Promises.

125. Defendant's privacy policies represent to Plaintiff and Class Members that Defendant will keep PHI and PII private and confidential and Beaumont will only disclose PHI under certain circumstances.

126. Beaumont's Notice of Privacy Practices represents to patients and Website visitors that Defendant will keep PHI confidential and will only disclose it under certain circumstances,

none of which apply here.³¹

127. Defendant affirmatively represents that “*[w]e will only use your health information for purposes specifically allowed by federal and state laws or regulations unless you provide written authorization. If your health information is sought for a use that requires your written authorization, you will be told the reason for the request, who is asking for the information and what information is requested.*”³²

128. Beaumont’s Privacy Policy explains Defendant’s legal duties with respect to PHI and PII and the exceptions for when Defendant can lawfully use and disclose it.

129. The Privacy policy states, “Beaumont Health, the corporate parent to William Beaumont Hospital, Botsford General Hospital and Oakwood Healthcare, Inc., is committed to your right to privacy. For this reason, we have established website policies to protect the privacy of our website visitors. Any and all information collected on this website will be kept strictly confidential and will not be sold, reused, rented, loaned, traded, leased or otherwise disclosed without prior consent.”³³

130. Defendant’s Privacy Policy promises that Beaumont collects only ‘the domain name (e.g. xyz.com) of a visitor’s server’ and that ‘Beaumont collects very little personally identifiable information from visitors to its websites.’³⁴

131. Beaumont’s examples of how and where it collects PHI and PII do not include

³¹ *Joint Notice of Privacy Practices*, <https://www.beaumont.org/docs/default-source/privacy-notices/joint-notice-of-privacy-practices-booklet.pdf?sfvrsn=4> (last visited Sept. 27, 2024).

³² *Id.* (emphasis added).

³³ Beaumont Health’s Privacy Policy, <https://www.beaumont.org/patients-families/patients-rights-privacy/privacy> (last visited Sept. 27, 2024).

³⁴ *Id.*

patients' searches for specific medical conditions, treatments, providers, appointment details, nor does Defendant disclose that it will collect PHI and PII and send it to third-party data brokers, such as Meta, for marketing purposes.

132. Defendant's Privacy Policy does not permit Defendant to intercept, transmit, or disclose Plaintiff's and Class Members' PHI and PII to third parties, including Meta, for marketing purposes.

133. Defendant's Privacy Policy states that Defendant uses Google Analytics "that helps [Beaumont] understand how visitors engage with our Sites." But Google specifically advises its customers that they "must refrain from using Google Analytics in any way that may create obligations under HIPAA for Google. HIPAA-regulated entities using Google Analytics must refrain from exposing to Google any data that may be considered Protected Health Information (PHI), even if not expressly described as PII in Google's contracts and policies."³⁵

134. Defendant violated its own privacy policies by unlawfully intercepting and disclosing Plaintiff's and Class Members' PHI and PII to Meta and other third parties without adequately disclosing that it shares such information with third parties and without acquiring the specific patients' consent or authorization to share it.

F. Exposure of PHI and PII Creates a Substantial Risk of Harm.

135. The FTC has recognized that consumer data is a lucrative and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types

³⁵ *HIPAA and Google Analytics*, <https://support.google.com/analytics/answer/13297105?hl=en> ("[f]or HIPAA-regulated entities looking to determine how to configure Google Analytics on their properties, the HHS Bulletin provides specific guidance on when data may and may not qualify as PHI").

and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.”³⁶

136. The FTC also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require, among other things: (i) using industry tested and accepted methods; (ii) monitoring activity on networks to uncover unapproved activity; (iii) verifying that privacy and security features function properly; and (iv) testing for common vulnerabilities or unauthorized disclosures.³⁷

137. The FTC cautions businesses that failure to protect PHI and PII and the resulting privacy breaches can destroy consumers’ finances, credit history, and reputations, and can take time, money, and patience to resolve the effect.³⁸ Indeed, the FTC treats the failure to implement reasonable and adequate data security measures as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

G. Plaintiff’s and Class Members’ PHI and PII is Valuable.

138. As many health care data industry experts have recognized, “[p]atients’ medical data constitutes a cornerstone of the big data economy. A multi-billion dollar industry operates by

³⁶ *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, at 2 (Dec. 7, 2009) https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

³⁷ *Start With Security, A Guide for Business*, <https://www.ftc.gov/business-guidance/resources/start-security-guide-business>.

³⁸ See *Taking Charge: What to Do if Your Identity is Stolen*, FTC, at 2 (2012), <https://www.myocci.org/sites/default/files/pdf/taking-charge-1.pdf>.

collecting, merging, analyzing[,] and packaging patient data and selling it to the highest bidder.”³⁹

139. The personal, health, and financial information of Plaintiff and Class Members is valuable and has become a highly desirable commodity. One of the world’s most valuable resources is the exchange of personal data.⁴⁰

140. Business News Daily reported that businesses collect personal data (i.e., gender, web browser cookies, IP addresses, and device IDs), engagement data (i.e., consumer interaction with a business’s website, applications, and emails), behavioral data (i.e., customers’ purchase histories and product usage information), and attitudinal data (i.e., consumer satisfaction data) from consumers.⁴¹ Companies then use this data to impact the customer experiences, modify their marketing strategies, publicly disclose or sell data, and even to obtain more sensitive data that may be even more lucrative.⁴²

141. The power to capture and use customer data to manipulate products, solutions, and the buying experience is invaluable to a business’s success. Research shows that organizations who “leverage customer behavioral insights outperform peers by 85 percent in sales growth and

³⁹ Niam Yaraghi, *Who should profit from the sale of patient data?*, The Brookings Institution (Nov. 19, 2018), <https://www.brookings.edu/blog/techtank/2018/11/19/who-should-profit-from-the-sale-of-patient-data/>.

⁴⁰ *The world’s most valuable resource is no longer oil, but data* (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

⁴¹ Max Freedman, *How Businesses Are Collecting Data (And What They’re Doing With It)* (Aug. 5, 2022; updated May 30, 2023), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

⁴² *Id.*

more than 25 percent in gross margin.”⁴³

142. In 2013, the Organization for Economic Cooperation and Development (“OECD”) published a paper entitled “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value.”⁴⁴ There, OECD measured prices demanded by companies concerning user data derived from “various online data warehouses.”⁴⁵

143. OECD indicated that “[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., \$2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver’s license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55.”⁴⁶

144. Unlike financial information, such as credit card and bank account numbers, PHI and certain PII cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable.⁴⁷

145. Consumers place considerable value on their PHI and PII and the privacy of that

⁴³ Brad Brown, *et al.*, *Capturing value from your customer data* (Mar. 15, 2017), <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>.

⁴⁴ *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, OECD PUBLISHING PARIS (Apr. 2, 2013), <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

⁴⁵ *Id.* at 25.

⁴⁶ *Id.*

⁴⁷ *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters (July 21, 2020), <https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/>.

information.

146. Time Magazine published an article in 2017 titled “How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry” in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.⁴⁸

147. CNBC published an article in 2019 in which it observed that “[d]e-identified patient data has become its own small economy: There’s a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers.”⁴⁹

148. Marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. “No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable.”⁵⁰

149. Several companies have products through which they pay consumers for a license to track their data. For example, Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect pay for browsing historical information.

150. Facebook also has paid users for their digital information, including browsing history. Until 2019, Facebook ran a “Facebook Research” app through which it paid \$20 a month for a license to collect browsing history information and other communications from consumers between the ages of 13 and 35.

⁴⁸ See <https://time.com/4588104/medical-data-industry/>.

⁴⁹ See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html>.

⁵⁰ VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER <https://www.getvero.com/resources/twitter-lead-generation-cards/>.

151. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to \$250 per record on the black market.⁵¹

152. Defendant's privacy violations exposed a variety of PHI including patient status, health conditions and symptoms, physicians, and other highly sensitive data.

153. PHI, like that exposed here, is likely even more valuable than Social Security numbers and just as capable of being misused.⁵² PHI can be ten times more valuable than credit card information.⁵³ This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, prescriptions, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, Social Security numbers.⁵⁴

154. Some industry insiders and journalists are even calling hospitals the "brokers to technology companies" for their role in data sharing in the \$3 trillion healthcare sector.⁵⁵ "Rapid digitization of health records . . . have positioned hospitals as a primary arbiter of how much sensitive data is shared."⁵⁶

⁵¹ Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, SecureLink (June 30, 2021), <https://www.securelink.com/blog/healthcare-data-new-prize-hackers>.

⁵² *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), [https://publicintelligence.net/fbi-health-care-cyber-intrusions/#:~:text=\(U\)%20Cyber%20actors%20will%20likely,records%20in%20the%20black%20market](https://publicintelligence.net/fbi-health-care-cyber-intrusions/#:~:text=(U)%20Cyber%20actors%20will%20likely,records%20in%20the%20black%20market).

⁵³ Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

⁵⁴ *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

⁵⁵ Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records* (Jan. 20, 2020), <https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200>.

⁵⁶ *Id.*

H. Plaintiff and Class Members had a Reasonable Expectation of Privacy in their Interactions with Defendant's Web Properties.

155. Consumers assume the data they provide to hospitals will be kept secure and private.

156. In a survey related to Internet user expectations, most website visitors indicated that their detailed interactions with a website should only be used by the website and not be shared with a party they know nothing about.⁵⁷ Website visitors expect that their interactions with a website should not be released to third parties unless explicitly stated.⁵⁸

157. The majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its' customers' data.⁵⁹ A March 2000 BusinessWeek/Harris Poll found that 89 percent of respondents were uncomfortable with web tracking schemes where data was combined with an individual's identity.⁶⁰ The same poll found that 63 percent of respondents were uncomfortable with web tracking even where the clickstream data was not linked to personally identifiable information.⁶¹ A July 2000 USA Weekend Poll showed that 65 percent of respondents thought that tracking

⁵⁷ See *Privacy and Online Tracking Perceptions Survey Report* (March 2020), CUJOAI, at 15–19, Privacy Survey_03-24 (cujo.com) (indicating major concerns of survey respondents was illegal use of data and unethical tracking and indicating respondents' belief that responsibility allocation falls on websites, and Internet users should be able to turn to the websites themselves, for privacy breaches).

⁵⁸ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, THE INFORMATION SOCIETY, 38:4, 257, 258 (2022).

⁵⁹ *Public Opinion on Privacy*, EPIC.ORG, <https://archive.epic.org/privacy/survey/>.

⁶⁰ *Id.*

⁶¹ *Id.*

computer use was an invasion of privacy.⁶²

158. Patients and website users act consistently with their expectation of privacy. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.⁶³

159. Like the greater population, Defendant’s patients and prospective patients would expect the highly sensitive medical information they provided to Defendant through the Website to be kept secure and private.

I. Defendant’s Conduct Is Unlawful and Violated Industry Norms.

i. Defendant Violated HIPAA Standards

160. Under HIPAA, individuals’ health information must be:

properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well-being. The [Privacy] Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.⁶⁴

161. HIPAA “is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge.”⁶⁵ HIPAA requires appropriate administrative, physical, and technical safeguards to

⁶² *Id.*

⁶³ Margaret Taylor, *How Apple screwed Facebook* (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

⁶⁴ *Summary of the HIPAA Privacy Rule* (Oct. 19, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>.

⁶⁵ *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* (June 27, 2022), [https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20\(HIPAA\),-On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge](https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20(HIPAA),-On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge).

ensure the confidentiality, integrity, and security of electronic protected health information.⁶⁶

162. HIPAA defines PHI as “individually identifiable health information” that is “created or received by a health care provider” (or similar entities) that “[r]elates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.” 45 C.F.R. § 160.103.

163. Identifiers such as patient-status (i.e., information that connects a particular user to a particular health care provider), medical conditions, health symptoms, treatments, and physicians, gathered in this case by the Tracking Tools through Beaumont’s Website, constitute protected health information.

164. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data Defendant failed to protect.

165. As mentioned previously, HIPAA covered entities cannot share PHI or PII to online tracking technology vendors for marketing purposes without first obtaining the individual’s HIPAA-compliant authorization.⁶⁷

166. When a regulated entity, like Defendant, collects the individual’s information, that

⁶⁶ See *id.*

⁶⁷ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, *supra*, note 10. The HHS Bulletin also identifies several harms that may result from an impermissible disclosure of an individual’s PHI, including “identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual’s PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.” *Id.*

information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health, health care, or payment for care.

167. When Plaintiff communicated with Beaumont regarding "treatment options" and other health-related information on the Beaumont Website, the Tracking Tools intercepted and disclosed those communications to Meta and Google in violation of HIPAA's Privacy Rule.

ii. Defendant Violated Michigan Law

168. Michigan law has established policies and procedures for the maintenance, preservation, and storage of patient medical records.

169. Michigan law provides that all patients are entitled to privacy and confidentiality with respect to their treatment and medical records: "a health care corporation shall not disclose records containing personal data that may be associated with an identifiable member, or personal information concerning a member, to a person other than the member, without the prior and specific informed consent of the member to whom the data or information pertains. The member's consent shall be in writing." MCL 550.1406(1).

170. Michigan law also provides that medical professionals are not allowed to disclose information obtained from a patient: "a health care corporation shall make a disclosure for which prior and specific informed consent is not required upon the condition that the person to whom the disclosure is made protect and use the disclosed data or information only in the manner authorized by the corporation..... If a member has authorized the release of personal data to a specific person, a health care corporation shall make a disclosure to that person upon the condition that the person shall not release the data to a third person unless the member executes in writing another prior and specific informed consent authorizing the additional release." MCL 550.1406(1).

171. Defendant's actions described herein violated Michigan law.

iii. Defendant Violated Industry Standards

172. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

173. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

174. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care... Patient privacy encompasses a number of aspects, including, ... personal data (informational privacy)

175. AMA Code of Medical Ethics Opinion 3.2.4 provides:

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

176. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically...must...:(c) release patient information only in keeping with ethics guidelines for confidentiality.

CLASS ACTION ALLEGATIONS

177. Plaintiff brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and all others similar situated,

178. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All individuals residing in the United States whose PHI and PII was disclosed to a third party through Defendant's Web Properties without authorization or consent during the applicable statute of limitations period.

179. The Michigan Sub-Class that Plaintiff seeks to represent is defined as follows:

All individuals residing in the State of Michigan whose PHI and PII was disclosed to a third party through Defendant's Web Properties without authorization or consent during the applicable statute of limitations period.

180. The Nationwide Class and Michigan Sub-Class are collectively referred to as the Class.

181. **The following people are excluded from the Class:** (1) any Judge or Magistrate presiding over this action and members of their immediate families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors and any entity in which Defendant or its parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's and Defendant's counsel and (6) the legal representatives, successors and assigns of any such excluded persons.

182. Plaintiff reserves the right under Federal Rule of Civil Procedure 23 to amend or modify the Class to include a broader scope, greater specificity, further division into subclasses, or limitations to particular issues.

183. All members of the proposed Class are readily identifiable through Defendant's records.

184. All requirements for class certification under Fed. R. Civ. P. 23(a), 23(b)(2) and 23(b)(3) are satisfied.

185. **Numerosity.** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believe that the proposed Classes includes tens of thousands of people based on Beaumont's reported patient visits per year. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

186. **Commonality and Predominance.** This action involves common questions of law and fact to Plaintiff and Class Members, which predominate over any questions only affecting individual Class Members. These common legal and factual questions include, without limitation:

- a. Whether Plaintiff's and Class Members' private communications were intercepted, recorded, and disclosed;
- b. Whether the interception, recording, and disclosure of Plaintiff's and Class Members' communications was consensual;
- c. Whether Defendant owed Plaintiff and the other Class Members a duty to adequately protect their PHI and PII;
- d. Whether Defendant owed Plaintiff and the other Class Members a duty to secure their PHI and PII from interception and disclosure via third-party tracking technologies;
- e. Whether Defendant owed Plaintiff and the other Class Members a duty to implement reasonable data privacy protection measures because Defendant accepted, stored, created, and maintained highly sensitive information concerning Plaintiff and the Classes;
- f. Whether Defendant knew or should have known of the risk of disclosure of data through third-party tracking technologies;
- g. Whether Defendant breached its duty to protect the PHI and PII of Plaintiff and the other Class Members;
- h. Whether Defendant knew or should have known about the inadequacies of its privacy protection;
- i. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiff's and the Classes' PHI and PII from unauthorized disclosure;

- j. Whether proper data security measures, policies, procedures, and protocols were enacted within Defendant's computer systems to safeguard and protect Plaintiff's and the Classes' PHI and PII from unauthorized disclosure;
- k. Whether Defendant's conduct was the proximate cause of Plaintiff's and the Classes' injuries;
- l. Whether Plaintiff and Class Members had a reasonable expectation of privacy in their PHI and PII;
- m. Whether Plaintiff and Class Members suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;
- n. Whether Plaintiff and Class Members are entitled to recover damages; and
- o. Whether Plaintiff and Class Members are entitled to other appropriate remedies including injunctive relief.

187. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of herself and the Class. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

188. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI and PII, like that of every other Class Member, was improperly disclosed by Defendant. Defendant's misconduct impacted all Class Members in a similar manner.

189. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class and has retained counsel experienced in complex consumer class action litigation and intend to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Classes.

190. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. The adjudication of this

controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. Absent a class action, individual patients like Plaintiff would find the cost of litigating their claims prohibitively high and would have no effective remedy for monetary relief.

191. Class Certification under Fed. R. Civ. P. 23(b)(2) is also appropriate. Defendant has acted or refused to act on grounds that apply generally to the Class, thereby making monetary, injunctive, equitable, declaratory, or a combination of such relief appropriate. As Defendant continues to engage in the practices described herein, the risk of future harm to Plaintiff and the Class remains, making injunctive relief appropriate. The prosecution of separate actions by all affected individuals with injuries similar to Plaintiff's, even if possible, would create a substantial risk of (a) inconsistent or varying adjudications with respect to individual patients, which would establish potentially incompatible standards of conduct for Defendant, and/or (b) adjudications with respect to individual patients which would, as a practical matter, be dispositive of the interests of the other patients not parties to the adjudications, or which would substantially impair or impede the ability to protect the interests of the Class. Further, the claims of individual patients in the defined Class are not sufficiently large to warrant vigorous individual prosecution considering all of the concomitant costs and expenses.

TOLLING, CONCEALMENT & ESTOPPEL

192. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

193. Defendant secretly incorporated Tracking Tools into its Website, providing no

indication to users that their data, including their PHI and PII, would be disclosed to unauthorized third parties.

194. Defendant had exclusive knowledge that its Tracking Tools were incorporated on its Website yet failed to disclose that fact to patients and prospective patients or inform them that by interacting with its Web Properties Plaintiff's and Class Members' PHI and PII would be disclosed to third parties, such as Meta and Google.

195. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of Tracking Tools on Defendant's Web Properties is highly technical and there were no disclosures or other indications that would inform a reasonable consumer that Defendant was disclosing and allowing Meta or Google to intercept PHI and PII.

196. The earliest Plaintiff could have known about Defendant's conduct was approximately in August of 2024 when she discussed her potential claims with counsel. Nevertheless, at all material times herein, Defendant falsely represented to Plaintiff that her health information is not and will not be disclosed to any third party.

197. As alleged above, Defendant has a duty to disclose the nature and significance of its data disclosure practices but failed to do so. Defendant is therefore estopped from relying on any statute of limitations under the discovery rule.

LEGAL CLAIMS

COUNT I

Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1)
(By Plaintiff & on behalf of the Nationwide Class)

198. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully set forth herein.

199. The ECPA protects against intentional interception, attempted interception, or the procurement of another person to intercept or attempt to intercept any wire, oral, or electronic communication. *See* 18 U.S.C. § 2511(1)(a).

200. The ECPA protects both sending and receipt of communications.

201. The ECPA further provides any person who:

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

Shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

Id. §§ 2511(1)(c) & (d).

202. The primary purpose of the ECPA is to protect the privacy and security of communications as technology evolves.

203. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

204. Section 2520 provides for \$10,000 in statutory damages for violations of ECPA. *Id.* § 2520(c)(2)(B).

205. The ECPA defines “intercept[ion]” as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” *Id.* § 2510(4).

206. The ECPA defines “contents,” when used with respect to electronic

communications, to “include[] any information concerning the substance, purport, or meaning of that communication.” *Id.* § 2510(8).

207. “Electronic communication” means “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” *Id.* § 2510(12).

208. The transmissions of PII and PHI from Plaintiff and Class Members to Defendant through Defendant’s Web Properties are “electronic communications” under the ECPA. *See id.* § 2510(12).

209. The PHI transmitted by Plaintiff and Class Members include, but are not limited to, information regarding patient status, past and current health conditions and symptoms, treatments and care options, physicians, appointment details, location, and other sensitive information.

210. Furthermore, Defendant intercepted the “contents” of Plaintiff’s communications in at least the following forms:

- a. The parties to the communications;
- b. The precise text of patient search queries;
- c. PII such as patients’ IP addresses, Facebook IDs, browser fingerprints and other unique identifiers;
- d. The precise text of patient communications about specific doctors;
- e. The precise text of patient communications about specific medical conditions;
- f. The precise text of information generated when patients requested or made appointments;
- g. The precise text of patient communications about specific treatments;
- h. The precise text of patient communications about scheduling appointments with medical providers;

- i. The precise text of patient communications about billing and payment;
- j. The precise text of specific buttons on Defendant's Website that patients click to exchange communications including Log-Ins, Registrations, Requests for Appointments, Search and other buttons;
- k. The precise dates and times when patients click to Log-In on Defendant's Web Properties;
- l. The precise dates and times when patients visit Defendant's Web Properties;
- m. Information that is a general summary or informs third parties of the subject of communications that Defendant sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment and other information.

211. For example, Defendant's interception of the fact that a patient views a webpage

like:

- <https://www.beaumont.org/search-results?search=dermatologist>
- <https://www.beaumont.org/search-results?search=sleep%20study>
- <https://www.beaumont.org/services/sleep-evaluation-services>
- <https://www.beaumont.org/services/womens-services/maternity/after-pregnancy/breastfeeding/breastfeeding-lactation-consultants>
- <https://www.beaumont.org/services/womens-services/maternity/childbirth-parenting-education#newborn>

212. Additionally, through its use of the Tracking Tools, Defendant intercepted and disclosed the communications about patient status, health conditions and symptoms, and other PHI and PII Plaintiff searched for on Defendant's Web Properties. This information was, in turn, used by third parties, such as Meta and Google, to (i) place Plaintiff in specific health-related categories; and (ii) target Plaintiff with advertising associated with Plaintiff's particular health conditions. Defendant knowingly transmitted this data and did so for the purpose of financial gain.

213. "Electronic, mechanical or other device" means "any device or apparatus which can be used to intercept . . . electronic communication[s]." *Id.* § 2510(5).

214. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

- a. The cookies Beaumont, Meta, and Google use to track Plaintiff's and Class Members' communications;
- b. Plaintiff's and Class Members' browsers;
- c. Plaintiff's and Class Members' computing devices;
- d. Defendant's web servers; and
- e. The Meta Pixel and other Tracking Tools deployed by Defendant to effectuate the sending and acquisition of users' and patients' sensitive communications.

215. By embedding and deploying the Tracking Tools on Defendant's Web Properties, Defendant intentionally violated the ECPA, through its interception, attempt at interception, and its procurement of third parties to intercept the electronic communications of Plaintiff and Class Members.

216. Defendant also intentionally used or attempted to use the contents of Plaintiff's and Class Members' electronic communications, knowing that the information was obtained through interception. Defendant's use of the intercepted information and data for its own advertising and data analytics, in the absence of express written consent, violated ECPA.

217. Further, by embedding the Tracking Tools on its Web Properties and disclosing the content of patient communications relating to PHI and PII, without consent, Defendant had a purpose that was tortious, criminal, and designed to violate state and federal laws, including:

- a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;
- b. Violation of Section 5(a) of the FTC Act;
- c. Violation of the Michigan Public Health Code, MCL 333.20201(2)(c);
- d. Violation of the Michigan Nonprofit Health Care Corporation Reform Act, MCL 550.1406;
- e. Violation of the Michigan Consumer Protection act, MCL 445.903; and
- f. Invasion of Privacy.

218. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3).

219. 42 U.S.C. § 1320d-6(a)(3) provides criminal and civil penalties against a healthcare provider who “knowingly . . . discloses individually identifiable health information to another person.”

220. HIPAA defines IIHI as:

any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and*—(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.⁶⁸

221. HIPAA prohibits disclosing patients’ health information via tracking technologies. Defendant’s use of the Tracking Tools violates HIPAA because the Meta Pixel and the other Tracking Tools transmit information that “identifies the individual” or, at a minimum, “there is a reasonable basis to believe that the information can be used to identify the individual,” such as through unique identifying cookies and users’ IP addresses.

222. Defendant’s conduct violated 42 U.S.C. § 1320d-6 in that it: used and caused to be used cookie identifiers associated with specific patients without patient authorization; and

⁶⁸ U.S.C. § 1320d(6) (emphasis added).

disclosed IIHI to Facebook without patient authorization.

223. The penalty for violation is enhanced where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320d-6.

224. Defendant’s conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant’s use of the Facebook source code was for Defendant’s commercial advantage to increase revenue from existing patients and gain new patients.

225. As described above, Plaintiff entered data on Defendant’s Web Properties relating to health conditions and other PHI, and later received targeted advertisements from Beaumont. This shows that through the Tracking Tools employed, Defendant disclosed the IIHI of its Web Properties visitors to third parties in violation of the ECPA.

226. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendant’s invasion of privacy in learning that:

- a. Defendant intruded upon, intercepted, transmitted, shared, and used their PII and PHI (including information about medical symptoms, conditions, medical appointments, healthcare providers and locations, medications and treatments and health insurance and medical bills) for commercial purposes has caused Plaintiff and Class Members to suffer emotional distress;
- b. Defendant received substantial financial benefits from its use of Plaintiff’s and Class Members’ PII and PHI without providing any value or benefit to Plaintiff or Class Members;
- c. Defendant received substantial, quantifiable value from its use of Plaintiff’s and Class Members’ PII and PHI, such as understanding how people use its Web Properties and determining what ads people see on its Web Properties, without providing any value or benefit to Plaintiff or Class Members;
- d. Defendant failed to provide Plaintiff and Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of its patient information and
- e. The diminution in value of Plaintiff’s and Class Members’ PII and PHI and the loss

of privacy due to Defendant making sensitive and confidential information, such as patient status, medical treatment and appointments that Plaintiff and Class Members intended to remain private no longer private.

227. Patients have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that caused third-party Pixels and cookies (including but not limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on Plaintiff's and Class Members' computing devices as "first-party" cookies that are not blocked.

228. Defendant's scheme or artifice to defraud in this action consists of:

- a. the false and misleading statements and omissions in its privacy policy set forth above, including the statements and omissions recited in the claims below;
- b. the placement of the '_fbp' cookie on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Facebook, and
- c. the placement of the '_ga' and _gid cookies on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Google.

229. At no time did Plaintiff or Class Members consent to Defendant's disclosure of their PHI and PII to Meta, Google, or other third parties. Plaintiff and the Class had a reasonable expectation that Defendant would not re-direct their communications content to Meta, Google, or others attached to their personal identifiers in the absence of their knowledge or consent.

230. Any purported consent that Defendant received was not valid.

231. Defendant has improperly profited from its invasion of Plaintiff's and Class Members' privacy in its use of their data for its economic value.

232. Defendant knew that such conduct would be highly offensive. Regardless, it proceeded to embed the Tracking Tools and use them to the detriment of visitors to its Web

Properties.

233. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages and attorney's fees and costs.

COUNT II
Breach of Fiduciary Duty/Confidentiality
(By Plaintiff & on behalf of the Nationwide Class)

234. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully set forth herein.

235. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information. This duty arises from the implied covenant of trust and confidence that is inherent in the physician-patient relationship.

236. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website and Patient Portal.

237. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members: (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of disclosure of their Private Information to unauthorized third parties; and (3) to maintain complete and accurate records of what patient information (and where)

Defendant did and does store and disclose.

227. Contrary to its duties as a medical provider and its express and implied promises of confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

228. These disclosures were made for commercial purposes without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

229. The unauthorized disclosures of Plaintiff's and Class Members' Private Information were intentionally caused by Defendant's employees acting within the scope of their employment. Alternatively, the disclosures of Plaintiff's and Class Members' Private Information occurred because of Defendant's negligent hiring or supervision of its employees, its failure to establish adequate policies and procedures to safeguard the confidentiality of patient information, or its failure to train its employees to properly discharge their duties under those policies and procedures.

230. The third-party recipients included, but may not be limited to, Facebook and Google. Such information was received by these third parties in a manner that allowed them to identify the Plaintiff and the individual Class Members.

231. Defendant's breach of the common law implied covenant of trust and confidence is evidenced by its failure to comply with federal and state privacy regulations, including:

- a. By failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- b. By failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- c. By failing to ensure compliance with the HIPAA security standard rules by its

- workforce in violation of 45 C.F.R. § 164.306(a)(4);
- d. By failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiff's and Class Members PHI;
 - e. By failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
 - f. By failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);
 - g. By impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*;
 - h. By failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);
 - i. By failing to keep Private Information confidential as required by MCL 333.20201; and
 - j. By otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

232. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of private information and erosion of the essential confidential relationship between the healthcare provider and the patient.

233. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;
- b. Plaintiff and Class Members face ongoing harassment and embarrassment in the

- form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
 - d. General damages for invasion of their rights in an amount to be determined by a jury;
 - e. Nominal damages for each independent violation;
 - f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
 - g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
 - h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and
 - i. Defendant's actions violated the property rights Plaintiff and Class Members have in their Private Information.

COUNT III
Invasion of Privacy
(By Plaintiff & on behalf of the Nationwide Class)

238. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully set forth herein.

239. The PHI and PII of Plaintiff and Class Members consist of private and confidential facts and information that were never intended to be shared beyond private communications.

240. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PHI and PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

241. Defendant owed a duty to Plaintiff and Class Members to keep their PHI and PII confidential.

242. Defendant's unauthorized disclosure of Plaintiff's and Class Members' PHI and PII

to Meta and Google, two of the largest advertising companies, is highly offensive to a reasonable person.

243. Defendant's willful and intentional disclosure of Plaintiff's and Class Members' PHI and PII constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

244. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant facilitated Meta and Google's simultaneous collection and exploitation of confidential communications.

245. Defendant failed to protect Plaintiff's and Class Members' PHI and PII and acted knowingly when it installed the Tracking Tools onto its Web Properties because the purpose of the Tracking Tools is to track and disseminate individual's communications with the Web Properties for the purpose of marketing and advertising.

246. Because Defendant intentionally and willfully incorporated the Pixel and other Tracking Tools into its Web Properties and encouraged patients to use the Web Properties for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

247. As a proximate result of Defendant's acts and omissions, the private and sensitive PHI and PII of Plaintiff and Class Members was disclosed to a third party without authorization, causing Plaintiff and the Class to suffer damages.

248. Plaintiff, on behalf of themselves and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest and costs.

249. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PHI and PII is still maintained by Defendant and still in the possession of Meta and Google and the wrongful disclosure of the information cannot be undone.

250. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential PHI and PII. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook who on information and belief continues to possess and utilize that information.

COUNT IV
Breach of Implied Contract
(By Plaintiff & on behalf of the Nationwide Class)

251. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

252. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and the Class Members provided their Private Information and compensation for their medical care.

234. When Plaintiff and Class Members provided their Private Information to Defendant, they entered an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

235. Plaintiff and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

236. Plaintiff and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

237. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information without consent to third parties like Facebook or Google.

238. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

253. Plaintiff and Class Members are entitled to compensatory and consequential damages because of Defendant's breach of implied contract

COUNT V
Negligence
(By Plaintiff & on behalf of the Nationwide Class)

254. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

255. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

256. Upon accepting, storing and controlling the PHI and PII of Plaintiff and the Class, Defendant owed, and continues to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard, and protect their highly sensitive PHI and PII from disclosure to third parties.

257. As a medical provider, Defendant owed Plaintiff and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

258. Defendant had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed.

259. Defendant's duty to use reasonable security measures under HIPAA required

Defendant to “reasonably protect” confidential data from “any intentional or unintentional use or disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1).

260. Some or all of the healthcare, medical, or medical information at issue in this case constitutes “protected health information” within the meaning of HIPAA.

261. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

262. Defendant’s duty to use reasonable care in protecting confidential data also arose because Defendant is bound by industry standards to protect confidential PHI and PII.

263. Defendant breached its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff’s and Class Members’ PHI and PII from unauthorized disclosure.

264. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant’s Web Properties.

265. Contrary to its duties as a medical provider, Defendant negligently installed the Tracking Tools to disclose and transmit to third parties Plaintiff’s and Class Members’ communications with Defendant, including PHI and PII and the contents of such information.

266. These disclosures were made without Plaintiff’s or Class Members’ knowledge, consent, or authorization, and were unprivileged.

267. The third-party recipients included, but may not be limited to, Meta and Google.

268. As a direct and proximate cause of Defendant’s unauthorized disclosures of patient

personally identifiable, non-public medical information, and communications, Plaintiff and Class

Members were damaged by Defendant's breach in that:

- a. PHI and PII that Plaintiff and Class Members intended to remain private is no longer private;
- b. Plaintiff and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. Plaintiff and Class Members have suffered general and compensatory damages that were proximately caused by Defendant's negligence, in an amount to be determined by a jury;
- e. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- f. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- g. Defendant's negligent actions diminished the value of Plaintiff's and Class Members' PHI and PII; and
- h. Defendant's breach of its duties as a medical provider was the proximate cause of Plaintiff's and Class Members' injuries. But for Defendant's decision to install the invisible Tracking Tools on its Web Properties, Plaintiff's and Class Members' PHI and PII would not have been shared without their consent with Meta and other unauthorized third parties.

269. Defendant's wrongful actions and inactions and the resulting unauthorized disclosure of Plaintiff's and Class Members' PHI and PII constitutes negligence.

270. Plaintiff and Class Members are entitled to compensatory, nominal, and punitive damages in an amount to be determined at trial.

COUNT VI
Unjust Enrichment
(By Plaintiff & on behalf of the Nationwide Class)

271. Plaintiff realleges and incorporates by reference every allegation contained in the

paragraphs above as though fully stated herein.

272. Plaintiff pleads this claim in the alternative to their common law causes of action.

273. Plaintiff and Class Members conferred a benefit upon Defendant in the form of PHI and PII that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

274. Defendant benefits from the use of Plaintiff's and Class Members' PHI and PII and unjustly retained those benefits at their expense.

275. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

276. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members.

277. The services that Plaintiff and Class Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide.

278. The medical services Defendant offers are available from other health care systems that protect the confidentiality of patient communications. Had Defendant disclosed that it would allow third parties to secretly collect Plaintiff's and Class Members' PHI and PII without consent, neither s nor the Class Members would have purchased healthcare from Defendant.

279. By virtue of the unlawful, unfair, and deceptive conduct alleged herein, Defendant

knowingly realized revenue from the use of Plaintiff's and Class Members' PHI and PII for profit by way of targeted advertising related to their respective medical conditions and treatments sought.

280. It would be inequitable under unjust enrichment principles in Minnesota and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

281. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT VII
Violation of the Michigan Consumer Protection Act
MCL 445.901 *et seq.*
(By Plaintiff & on behalf of the Michigan Subclass)

282. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

283. Plaintiff and the Michigan Subclass are "persons" as defined by MCL § 445.903(d).

284. Defendant advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by MCL § 445.903(g).

285. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);
- b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);
- c. Making a representation or statement of fact material to the transaction such that a

person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb);

- d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

286. Defendant's unfair, unconscionable, and deceptive practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect the Private Information of Plaintiff and the Michigan Subclass, which was a direct and proximate cause of the improper disclosure of Plaintiff's and the Michigan Subclass' PHI to unauthorized third parties like Facebook and Google;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures to prevent unlawful disclosure of Plaintiff's and the Michigan Subclass' PHI by the Tracking Tools embedded on its Website;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiff and the Michigan Subclass, including duties imposed by HIPAA and the FTC Act, which was a direct and proximate cause of the improper disclosure of their PHI to Facebook;
- d. Misrepresenting that it would protect the privacy and confidentiality of the Private Information of Plaintiff and the Michigan Subclass, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiff and the Michigan Subclass, including duties imposed by HIPAA and the FTC Act;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure the Private Information of Plaintiff and the Michigan Subclass; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiff and the Michigan Subclass, including duties imposed by HIPAA and the FTC Act.

287. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of its users' and patients' Private Information.

288. Defendant intended to mislead Plaintiff and the Michigan Subclass and induce them to rely on its misrepresentations and omissions.

289. Defendant acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded the rights of Plaintiff and the Michigan Subclass.

290. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff and the Michigan Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; loss of value of their Private Information; and ongoing harassment and embarrassment in the form of unwanted targeted advertisements.

291. Plaintiff and the Michigan Subclass seek all monetary and nonmonetary relief allowed by law, including the greater of actual damages or \$250, restitution, injunctive relief, and any other relief that is just and proper.

COUNT VIII
Violation of the Michigan Nonprofit Health Care
Corporations Reform Act
MCL §550.140 *et seq.*
(By Plaintiff & on behalf of the Michigan Subclass)

292. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

293. This cause of action is brought pursuant to the Michigan Nonprofit Health Care Corporation Reform Act (the "Reform Act"), MCL § 550.140, which requires in relevant part that a Michigan nonprofit healthcare corporation "use reasonable care to secure" members' healthcare

records “from unauthorized access” and thereby “ensure the confidentiality of records containing personal data that may be associated with identifiable members.” MCL 550.1406(1).

294. As a nonprofit healthcare corporation incorporated in the State of Michigan and providing healthcare and hospital services in the State, Beaumont is and was at all relevant times a “healthcare corporation” as that term is defined in MCL §§ 550.1105(2) and 50.1406.

295. As a person entitled to receive healthcare under a nongroup insurance certificate while obtaining healthcare from Beaumont, Plaintiff is and was at all relevant times a “member” as that term is defined in MCL §§ 550.1106(3) and 50.1406.

296. By the acts alleged above, Beaumont violated the Reform Act by failing to adequately safeguard Plaintiff’s PII/PHI from unauthorized access by third party actors. Considering the sensitivity of the information Beaumont possessed, Beaumont was aware or should have been aware of the need to implement robust security measures to protect such information. It consciously refused to do so.

297. Accordingly, Plaintiff and each member of the Michigan subclass are entitled to, and seek, damages “for a violation of [the Reform Act] and may recover actual damages or \$200.00, whichever is greater, together with reasonable attorneys’ fees and costs.” § 550.1406(4).

REQUEST FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for judgment in their favor as follows:

- a. Certification of the Class pursuant to the provisions of Fed. R. Civ. P. 23 and an order that notice be provided to all Class Members;
- b. Designation of Plaintiff as representatives of the Class and the undersigned counsel as Class Counsel;
- c. An award of damages in an amount to be determined at trial or by this Court;

- d. Declaring that Defendant's past conduct was unlawful, as alleged herein;
- e. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;
- f. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;
- g. Awarding Plaintiff and Class Members statutory, actual, compensatory, consequential, and nominal damages, as well as restitution and disgorgement of profits unlawfully obtained;
- h. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest;
- i. Awarding Plaintiff and Class Members reasonable attorneys' fees, costs, and expenses; and
- j. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: November 14, 2024

Respectfully submitted,

s/ David S. Almeida

David S. Almeida
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
T: (312) 576-3024
E: david@almeidalawgroup.com

Attorneys for Plaintiff & the Putative Class